WebTrafficParser formParameter Option NS LocationAPI karakteriseren

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Voorbeeld #1: Verkeersprofiel

Conclusie

Gerelateerde informatie

Inleiding

Dit document beschrijft het filteren van LocationAPI met webTrafficParser tegen access_log HTTP POST formParameter, aangezien NS 2024.01 HTTP GET is verwijderd.

Cisco raadt kennis van de volgende onderwerpen aan:
- Cisco BroadWorks System Administrator-privilege.
- NS Locatie en Portal API Verzoeken Reactie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot speciale software- en hardwareversies.
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De locatie-API-aanvraag/reactie kan worden gevolgd als HTTP GET-aanvraaglogrecord in Cisco BroadWorks Network Server tomcat access_log. Deze methode werd in de functie 2024.01 vervangen door HTTP POST. Bij deze wijziging heeft het logboek voor toegang tot tomcat het veld FormParameters toegevoegd. De ingebouwde BroadWorks webTrafficParser is sindsdien verbeterd om dit veldParameters te filteren en te lezen. U kunt LocationAPI-probleem identificeren door het NS tomcat-toegangslog met webTrafficParser te plakken en te analyseren om te identificeren vanuit het HTTP POST-verzoek en het bijgevoegde formParameter-veld.

Voorbeeld #1: Verkeersprofiel

De tool webTrafficParser bevindt zich in de bin-directory (/user/local/broadworks/bw_base/bin):

bwadmin@ns$ CD /USR/Local/Broadworks/BW_BASE/BIN
bwadmin@ns$ ls -ltr webTrafficParser

lrwxrwx. 1 bworks bwadmin 58 apr 15 13:16 webTrafficParser ->
../../apps/WebContainer_2026.02_1.261/bin/webTrafficParser

bwadmin@ns$ webTrafficParser

Moet een of meer logbestanden opgeven.

Gebruik:

webTrafficParser [-a] [-m <regexp>] [-r] [-p <interval>] [-t <nummer>] <naam(en) van het logbestand>

Deze tool parseert toegang tot kattenlogs om binnenkomend verkeer te karakteriseren.

Lijst met mogelijke opties:

-A: drukt volledige uitvoer af (alle vermeldingen in plaats van top 10)

-m <regexp> : hiermee worden logbestandsindelingen afgedrukt die overeenkomen met reguliere expressie

-r: geeft op snelheid gebaseerde (berichten per seconde) informatie weer

-t <nummer> : drukt bovenste <nummer> items af

-s <Start_time> : begintijd voor bestand(en). Voorbeeld formaat voor tijden 30/Jan/2013:19:22:57

Standaard op eerste keer in bestand(en).

-e <End_time> : eindtijd voor bestand(en). Standaard de laatste keer in het laatste bestand.

-p <interval> : drukt een verkeersprofiel af van begin- tot eindtijd met een interval

(in minuten). Dit kan worden opgeslagen in een CSV-bestand en gegraveerd.

Het script parseert maximaal 10 logbestanden.

De namen van de logbestanden moeten in tijdvolgorde worden opgegeven.

Plak het NS-toegangslogboek van een focustijdframe naar webTrafficParser, dit geeft een hoog volume terug voor een bepaald gebruiker Locatie API-verzoek (416 in totaal):

- bwadmin@ns$ webTrafficParser access_log.2026.10*.txt

  ns1-r25.cisco.com HET VERKEER TELT. STARTTIJD = 01/okt/2026:00:00:49. EINDTIJD = 08/okt/2026:21:09:09.

Totale tijd = 677300.000 seconden
Totaal aantal aanvragen = 33996

68 Gemiddelde aanvraaggrootte (bytes)
641 Gemiddelde responsgrootte (bytes)
0,002 Gemiddelde responstijd (seconden)

Verkeer volgens HTTP-methode:
22994 POST
6105 GET
4599 OPTIES
251-
9 HOOFD
8 GNUTELLA
4 Sommige
4 NESSUS
4 PROPFIND
4 SPOREN

Top 10 van URL's:
22389
/servlet/GetAllHostingNeNodeAddresses?private=false&broadworksOnly=true&clusterMode=false&callPRequest=true&request
Adressen=10.66.82.113
4599 *
781/
416 /servlet/LocateUser?url=jliangEntGrp1User5%40syd.cisco.com&returnCompatibleXSP=true&callPRequest=true
251-
126 /Inloggen/
92 /Aanmelden
88 /afbeeldingen

52 /login.html
38 /index.html

Top 10 op adres:
22833 10,66,82,113
4587 10,66,82,105
3288 <een openbaar IP-adres>
3288 <Een ander openbaar adres>

Top 10 van de retourcode:
27554 200
5077 302
804 404
553 400
4 403
4 405

Top 10 op gebruikersnaam:
33996-

Top 10 door user-agent:
..

bwadmin@ns$

Plak de userId 'jliangEntGrp1User5' als parameter van de -m optie op webTrafficParser. Dit retourneert de specifieke userId in veld 15 van de toegangslogboekvermeldingen. Veld 15 is formParameters van het HTTP POST-verzoek.

```
bwadmin@ns$ CD /var/Broadworks/Logs/Tomcat/
bwadmin@ns$ webTrafficParser -m "jliangEntGrp1User5" access_log.2026.10*.txt
10.66.82.113 - [01/okt/2026:10:34:24 +1000] "POST /servlet/LocateUser HTTP/1.1" 200 94 199 0.003 3 "
220f25f7-7353-4d4b-960a-4b3136897297" 10.66.82.115 80
"url=jliangEntGrp1User5&returnCompatibleXSP=true&callPRequest=false&netadmin=jli
angEntGrp1User5"
..
10.66.82.113 - [08/okt/2026:21:28:04 +1100] "POST /servlet/LocateUser HTTP/1.1" 200 126 199 0.002 2
"COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8" 10.66.82.115 80
"url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=j
bwadmin@ns$
```

U kunt doorgaan naar de volgende stap om de NSPortalLog te analyseren. Wijzig in de directory voor het registreren van de gegevens. U plakt de parameter userId jliangEntGrp1User5 als -m aan bwTrafficParser om de nsportallog te analyseren. Dit resulteert in een locatie API probleem, waarbij de NS de gebruikersnaam niet kan vinden: jliangEntGrp1User5@cisco.com:

- bwadmin@ns$ CD /var/Broadworks/Logs/Nsportal/
  bwadmin@ns$ bwTrafficParser -m "jliangEntGrp1User5" NSPortalLog2026.10.08-00.00.03.txt
  2026.10.08 21:28:04:536 AEDT | Info | HTTP | HTTPThread-49 | 7669459 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

  tcp - HTTP Bytes IN vanaf 10.66.82.113:57078 (ontvangen op 10.66.82.115:80)
  POST http://10.66.82.115/servlet/LocateUser
  Koppen:
  TrackingID: COMMPILOT_64DADD43-BA66-4805-B397-ABD3A7D512A8
  X-Broadsoft-Correlation-ID: CC6F959B-2507-4792-B158-780C74AF0D07
  X-Broadworks-Protocol-versie: 1.1
  Inhoudstype: toepassing/x-www-form-urlencoded
  Charset: UTF-8
  ..
  Verhuurder: 10.66.82.115
  Accepteer: tekst/HTML, afbeelding/GIF, afbeelding/JPEG, */*; q=0.2
  Verbinding: in leven houden
  Inhoudslengte: 126
  Parameters:
  URL=jliangEntGrp1User5@sys.cisco.com

returnCompatibleXSP=true
callPRequest=false
netadmin=jliangEntGrp1User5@sys.cisco.com

bwadmin@ns$ bwTrafficParser -m COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8 NSPortalLog2026.10.08-00.00.03.txt
2026.10.08 21:28:04:536 AEDT | Info | HTTP | HTTPThread-49 | 7669459 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp - HTTP Bytes IN vanaf 10.66.82.113:57078 (ontvangen op 10.66.82.115:80)
POST http://10.66.82.115/servlet/LocateUser
Koppen:
TrackingID: COMMPILOT_64DADD43-BA66-4805-B397-ABD3A7D512A8
X-Broadsoft-Correlation-ID: CC6F959B-2507-4792-B158-780C74AF0D07
X-Broadworks-Protocol-versie: 1.1
Inhoudstype: toepassing/x-www-form-urlencoded
Charset: UTF-8
user-agent: Java/11.0.29
Verhuurder: 10.66.82.115
Accepteer: tekst/HTML, afbeelding/GIF, afbeelding/JPEG, */*; q=0.2
Verbinding: in leven houden
Inhoudslengte: 126
Parameters:
URL=jliangEntGrp1User5@sys.cisco.com
returnCompatibleXSP=true
callPRequest=false
netadmin=jliangEntGrp1User5@sys.cisco.com

2026.10.08 21:28:04:536 AEDT | Foutopsporing | Algemeen | HTTPThread-49 | 7669460 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

doFilter()

2026.10.08 21:28:04:536 AEDT | FieldDebug | PortalInputChannel | HTTPThread-49 | 7669461 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

Aanvraag accepteren met versie: 1.1 (server op 1.1)

2026.10.08 21:28:04:537 AEDT | Info | LocationAPI | HTTPThread-49 | 7669462 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp 188 HTTP-bytes NAAR 10.66.82.113:57078 (verzonden vanaf 10.66.82.115:80)
<?xml version="1.0" encoding="UTF-8"?>

<com.broadsoft.protocols.nsportal.Error detail="Onbekende URL"
ID="2"
summary="Aanvraag kan niet worden voltooid"
>
</com.broadsoft.protocols.nsportal.Error>

2026.10.08 21:28:04:537 AEDT | Info | HTTP | HTTPThread-49 | 7669463 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp - HTTP Bytes UIT naar 10.66.82.113:57078 (verzonden vanaf 10.66.82.115:80)
statusCode=200
Koppen:

```
X-Content-Type-Opties: niet-snuiven
X-XSS-bescherming: 1; modus=blok
Tracking-ID: COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
X-BROADSOFT-CORRELATIE-ID: cc6f959b-2507-4792-b158-780c74af0d07
X-BroadWorks-Protocol-Versie: 1.1
Content-Type: tekst/html; charset=UTF-8
Overdracht-codering: gehakt
Datum: do, 08 okt 2026 10:28:04 GMT
Keep-Alive: time-out=5
Verbinding: in leven houden
Server: HTTP-server
```

Conclusie

Na deze probleemoplossing om de LocationAPI te identificeren 'Onbekende URL' is de hoofdoorzaak van een hoog bedrag van 200 OK voor HTTP POST met formParam

"url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=jl
kunt u controleren of de gebruikersnaam jliangEntGrp1User5@cisco.com alleen in AS bestaat vanwege een SyncAPI-probleem.

Gerelateerde informatie

- RemoveSensitiveInformationFromNSLocationAndPortalAPIRequestsFD-R2024_01.pdf

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.